Energy 2023, March 13-17, 2023 - Barcelona, Spain

Cybersecurity in Power Systems

A view on regulation and standardization

Steffen Fries, Siemens, T CST

SIEMENS

Abstract

Power systems as one critical infrastructure demand specific consideration regarding their reliable and resilient operation. Cybersecurity is one functionality supporting this operation and is increasingly demanded by regulation.

To cope with these requirements, different standard (frameworks) have been developed. They address technical and procedural requirements as well as technical specifications to ensure interoperability between different vendors products. Moreover existing standards are renewed or enhanced to address upcoming requirements and advances in cybersecurity.

The presentation provides an overview of regulative requirements and solution standards ensuring secure operation of the electrical infrastructure. Besides this, examples are provided for challenges, requiring further investigation and solution discussion and development.

SIEMENS

Businesses and Services of Siemens AG

Industrial Business

Digital Industries

Smart Infrastructure

Mobility

Siemens Healthineers[1]

Portfolio Companies

Siemens Advanta

Services

Siemens Financial Services

Siemens Real Estate

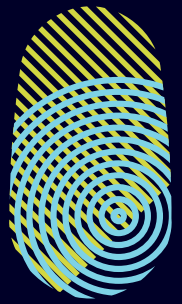
Global Business Services

1 Publicly listed subsidiary of Siemens; Siemens' share in Siemens Healthineers is 75%

SIEMENS

Charter of Trust
A joint initiative for a secure sustainable digital world

aes AIRBUS Allianz Atos BOSCH
DELL Technologies Deutsche Post DHL Group IBM Infineon Microsoft
MITSUBISHI HEAVY INDUSTRIES, LTD. msc NTT NXP SGS
TotalEnergies SIEMENS TÜV SÜD



Charter of Trust
charteroftrust.com

Associated Partner Forum

Bundesamt für Sicherheit in der Informationstechnik
CANADIAN CENTRE FOR CYBER SECURITY
CEBRI
CCN Centro Criptológico Nacional
CYBER READINESS INSTITUTE
CyberPeace Institute
GLOBAL CYBER ALLIANCE
HPI Hasso Plattner Institut
METI
総務省 MIC Ministry of Internal Affairs and Communications
TU Graz

01
Protect the data of individuals and businesses

02
Prevent damage to people, businesses, and infrastructure

03
Build trust in the digital world

SIEMENS

Company Core Technologies
Innovation examples

Simcenter ROM Builder

- Creation of simplified, tool-neutral and reusable models by processing simulation and field data
- Model generation accelerated (up to real-time), interoperable, and deployable from simulation to edge and cloud

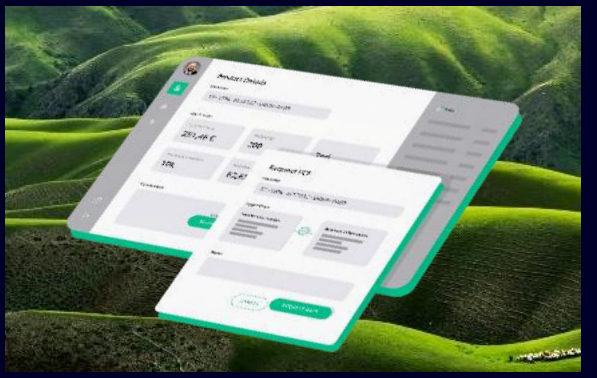
OT Security Appliance (OSA)

- Comprehensive asset discovery and security monitoring of industrial automation networks and applications
- On-site security monitoring during ongoing industrial operations and AI for behavior-based anomaly detection

Reliable power with renewable generation

- Assistant for power system operation with up to 100% renewable peak generation
- Collaborative stabilization and resilience of entire island grids (e.g. Hawaii)
- Capacity can be scaled up to a range between 100 MW and 100 GW

SiGREEN

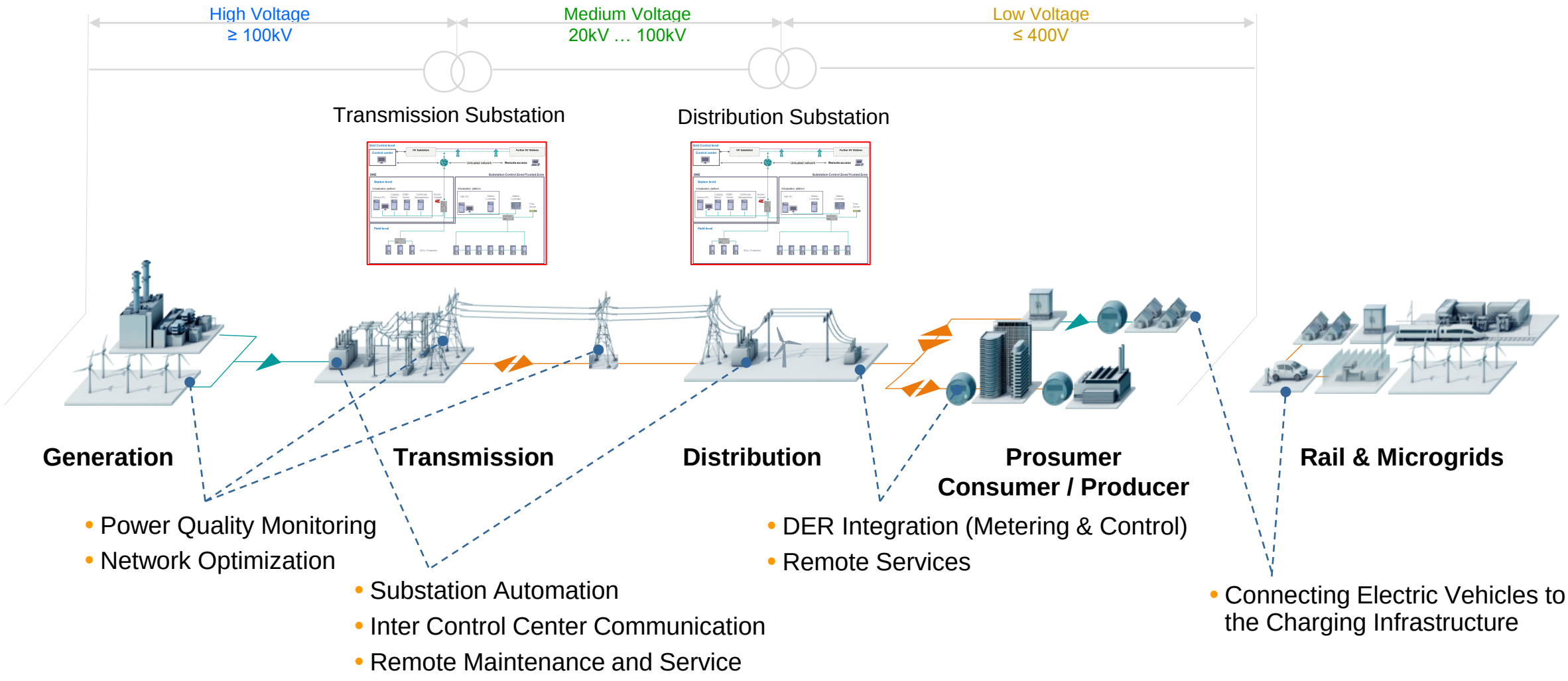


- Trustworthy exchange of actionable Product Carbon Footprints throughout value chains
- Use of verifiable credentials ensures transparency, confidentiality, and data control in supply chains

SIEMENS

Digital Grid – a Critical Infrastructure in Need of Protection

Power system value chain and use case examples



SIEMENS

Security must be (continuously) adopted to the changing threat and vulnerability landscape

1950s – 1960s
Military, governments and other organizations implement computer systems

1970s
Home computer is introduced

1980s
Computers make their way into schools, homes, business and industry

1990s
Digital enhancement of electrification and automation

1999
The globe is connected by the internet

1991
The World Wide Web becomes publicly accessible

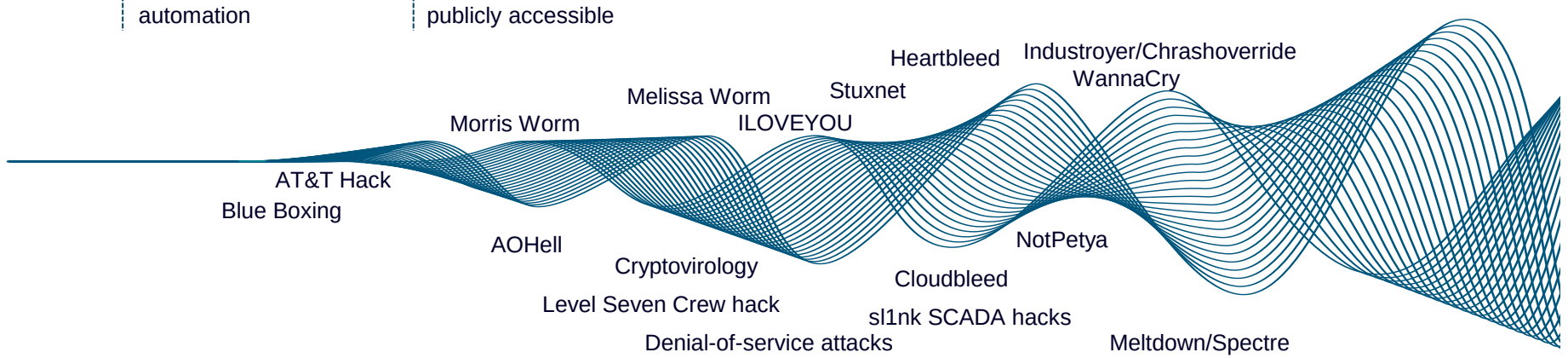
2010s
Cloud computing enters the mainstream

2000s
Mobile flexibility

2020s
Internet of Things, Smart and autonomous systems, Artificial Intelligence, Big Data

2020s
Industry 4.0

Digital Information Processing | Digital Connectivity | Digital Automation and Artificial Intelligence



SIEMENS

How to provide appropriate cybersecurity?

Cybersecurity needs a holistic methodology

Recover

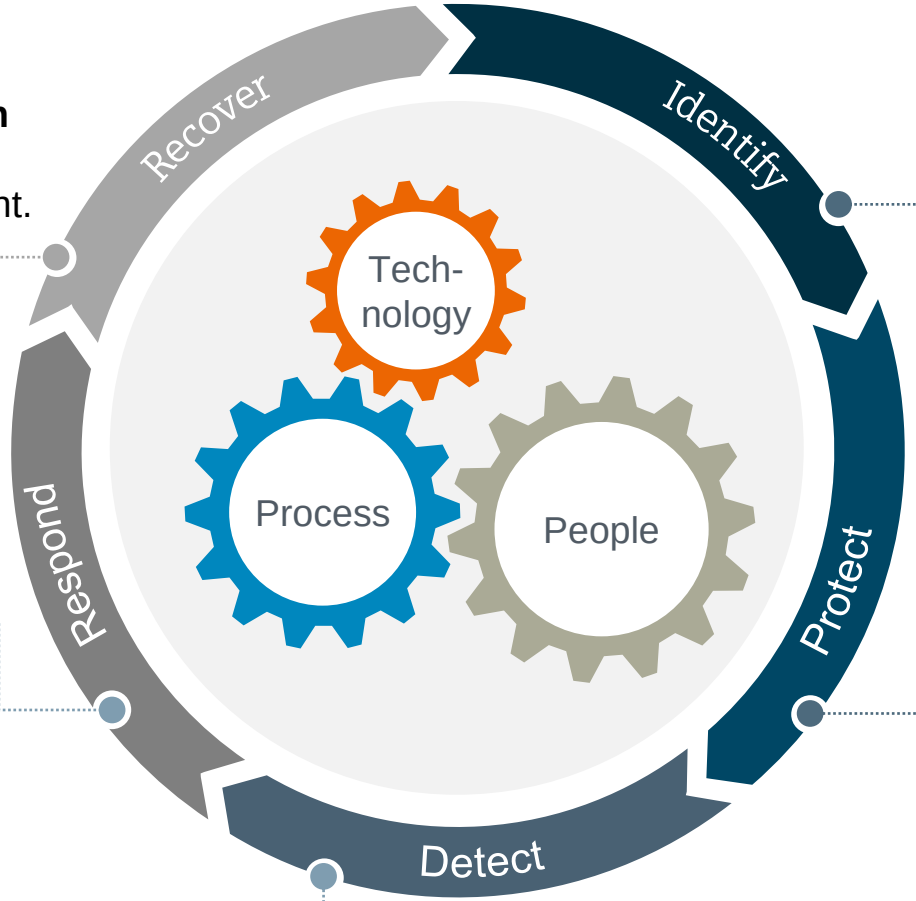
Creating plans for resilience and **restoration** of any capabilities or services that were impaired due to a cyber security related event.

Respond

Taking action against detected cyber security related events. Supports the ability to contain the impact of a potential event.

Detect

Rapid **identification** of the occurrence of a cyber security related event.



Identify

Understanding the business context, the resources that support critical functions and the related cyber security risks.

Protect

Protection of critical infrastructure service, e.g., energy supply by safeguarding the overall system.

The Five Functions are part of the NIST Cyber Security Framework

SIEMENS

Digital Grid as critical infrastructure is addressed through regulative requirements and standards (examples, global view)

Regulative Requirements

Homeland Security · NERC · FERC

- Critical Infrastructure Protection (NERC CIP)
- Executive Order 13636 improving Critical Infrastructure Cyber Security
- Executive Order 14028 improving Nation's Cyber Security

Bundesamt für Sicherheit in der Informationstechnik

- IT Security Act
- B3S Standards
- BNetzA Security Catalogue
- German Energy Act

- Cyber Security Act (CSA)
- Network Information Security Directive (NIS2)
- Cyber Resilience Act (CRA)

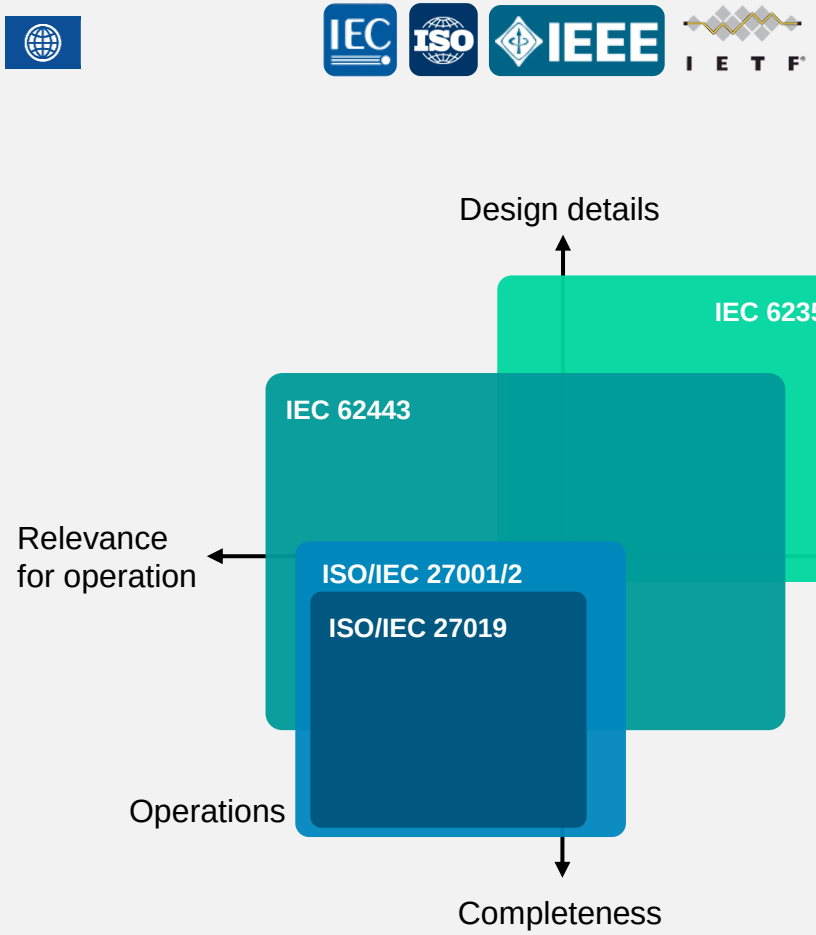
ANSSI – Agence nationale de la sécurité des systèmes d'information

- Critical Infrastructure Protection
- Certification and Key Measures

CPNI – Centre for the Protection of National Infrastructure

- Cyber Essential Scheme
- Direct adaptation of European NIS Directive and GDPR

International Standards



Note: the stated organizations and standards are just examples and are not complete

SIEMENS

ISO/IEC 270xx Series – Information Security Management System (ISMS)

Specifies security management requirements for manufacturers, operators, …

ISMS Family of standards

Vocabulary standard	**27000** Overview and vocabulary	
Requirement standards	**27001** ISMS – Requirements	**27006** Requirements for bodies providing audit and certification of ISMS
Guideline standards	**27002** Code of practice for information security controls	**27005** Information security risk management
	27003 ISMS – Implementation guidance	**27007** Guideline for ISMS auditing
	27004 ISMS – Measurement	
Sector-specific guideline Standard (exmples)	**27017** Code of practice for information security controls based on ISO/IEC 27002 for cloud services	**27019** ISMS – Guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Addresses specifically

- Security Policies
- Organization and info. security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environ. Security
- Operations Security
- Communications Security
- System and Application
- Supplier Relationship
- Incident Management
- Business Continuity
- Compliance

Domain specific standards augment ISO 27002 according to the target environment

SIEMENS

IEC 62443 – Security for Industrial Automation and Control Systems

Addresses the complete value chain from product manufacturing to operation

- Targets operator, integrator, and product supplier in terms of processes and security capabilities and allows for certification

General	Policies & Procedures	System	Component / Product	Profiles	Evaluation
1-1 Terminology, concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure Product Development Lifecycle Requirements	5-x Profile x	6-1 Security Evaluation Methodology for IEC 62443-2-4
1-2 Master glossary of terms and abbreviations	2-2 IACS Security Protection	3-2 Security Risk Assessment for System Design	4-2 Technical security requirements for IACS components		6-2 Security Evaluation Methodology for IEC 62443-4-2
1-3 Performance metrics for IACS security	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels			
1-4 IACS security lifecycle and use-cases	2-4 Security program requirements for IACS service providers				
1-5 Scheme for IEC 62443 Cyber Security Profiles	2-5 Implementation guidance for IACS asset owners				

Selected Certificates issued to Siemens

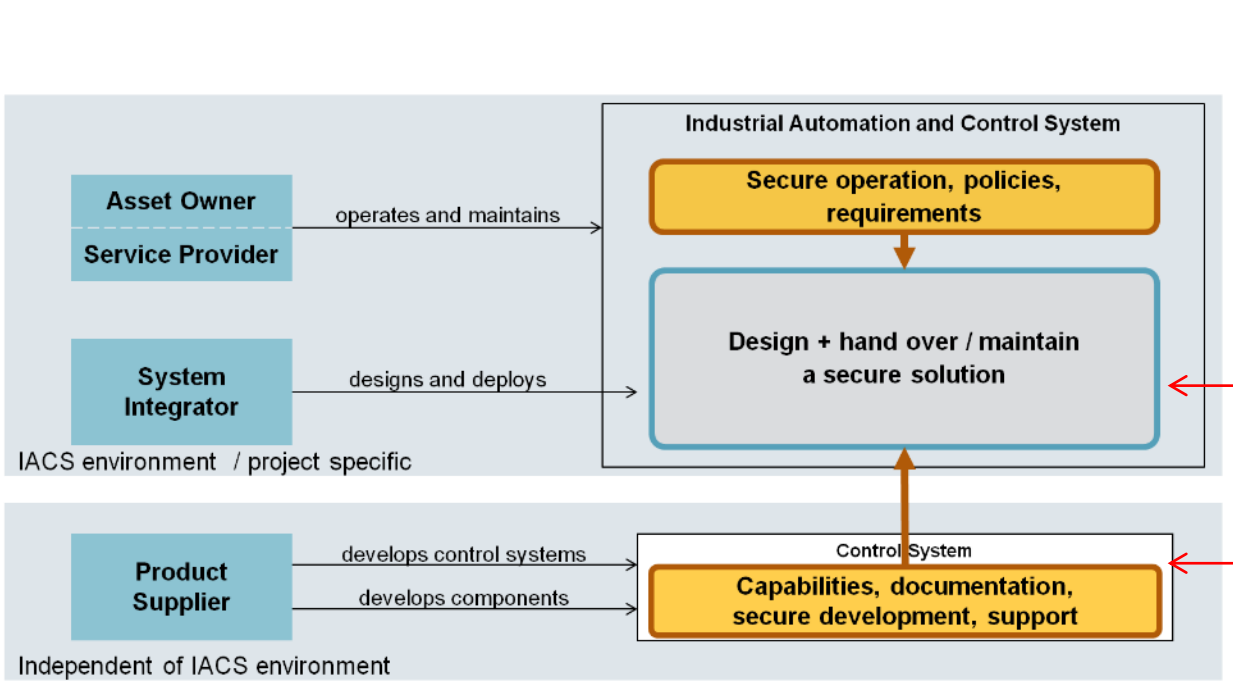
Certification relevance
Functional
Procedural

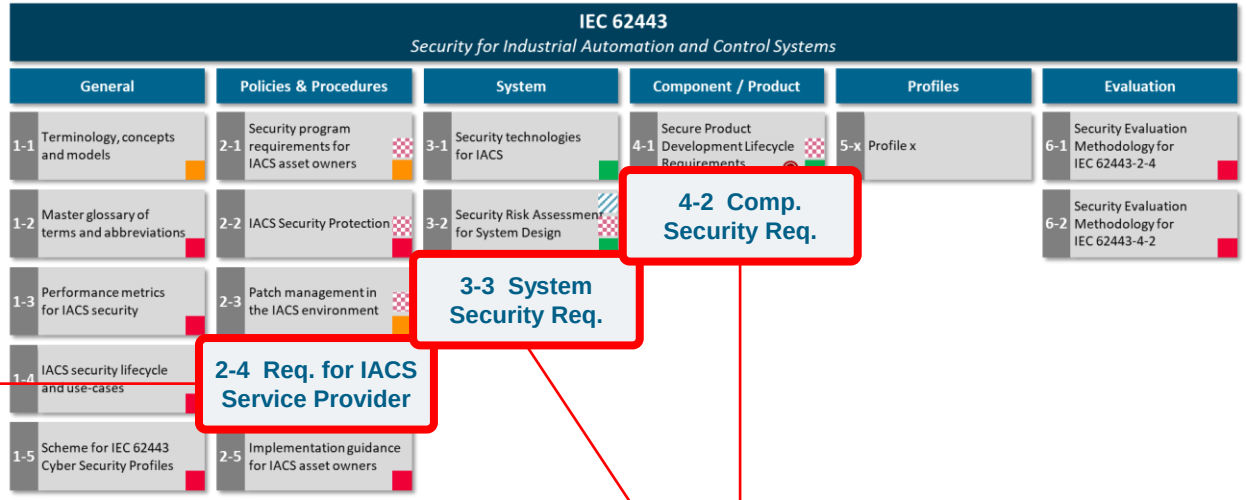
Published
Under revision
In development / planned

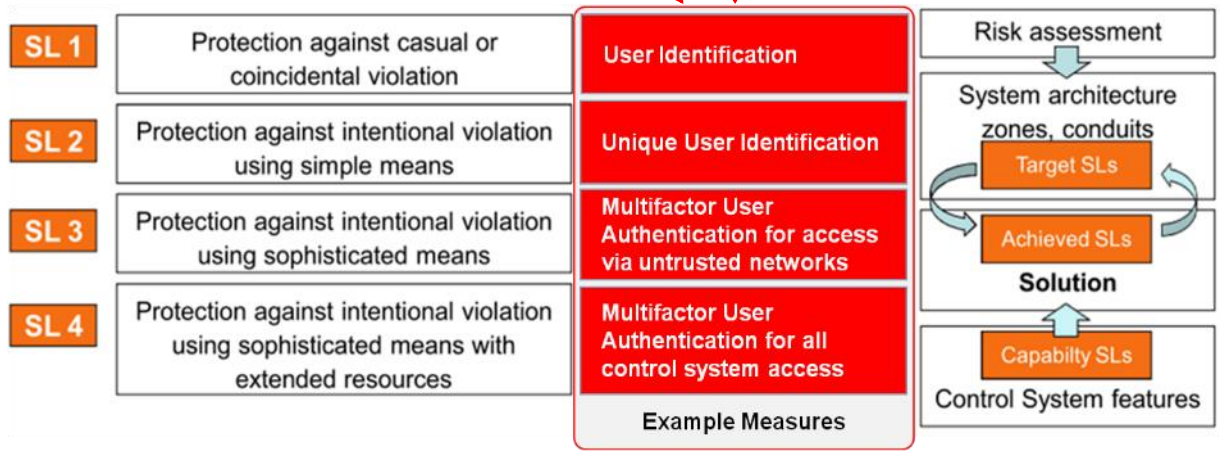
SIEMENS

IEC 62443 – Security for Industrial Automation and Control Systems

Enables a graded security approach to achieve appropriate protection







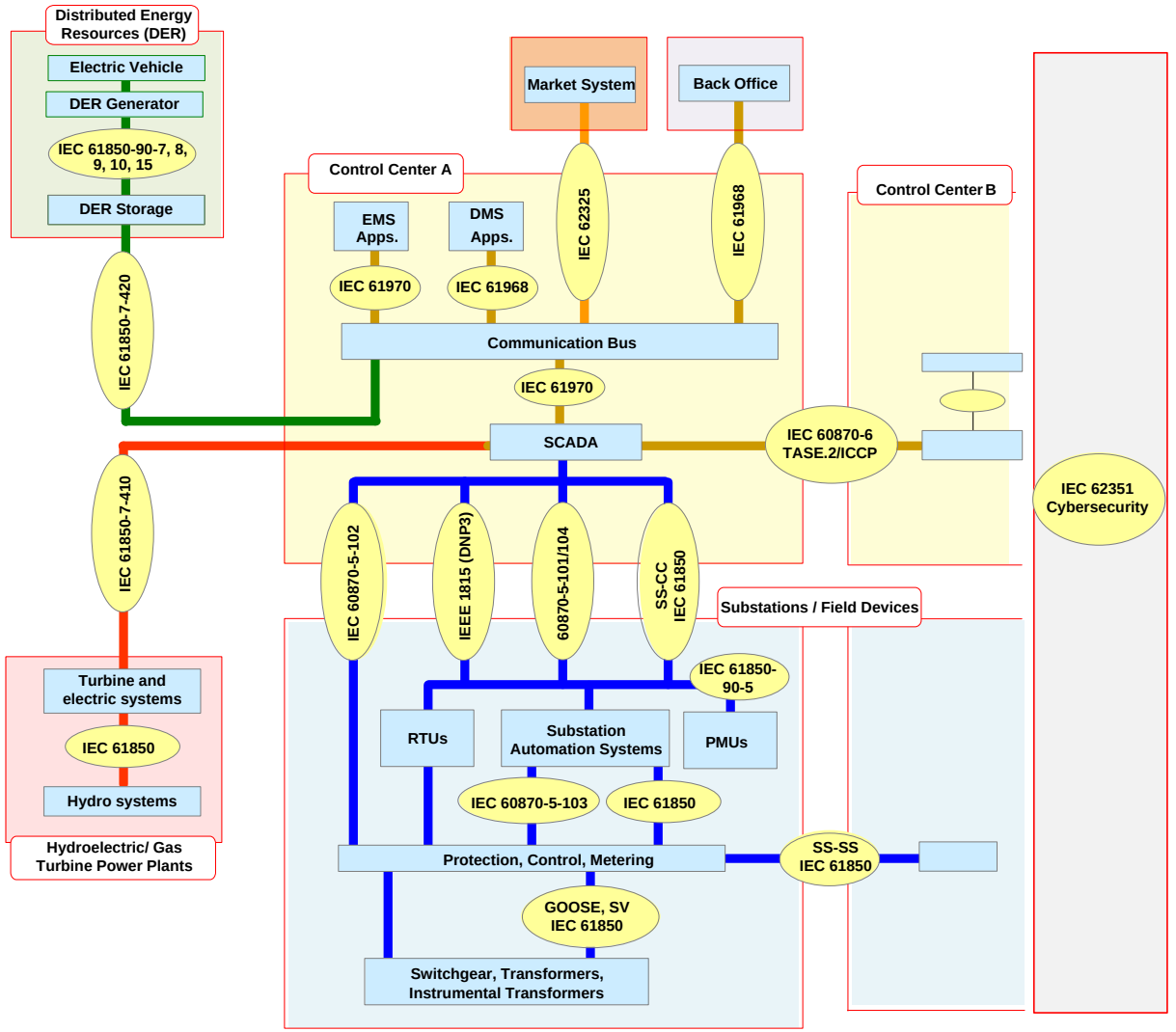
SIEMENS

Core Communication Standards for Digital Grids

IEC TC57 defines the reference architecture with domain-specific cybersecurity

- Development of IEC 62351 to secure communication protocols defined by IEC TC 57, specifically
  - IEC 60870-5 and IEC 60870-6 series,
  - IEC 61850 series,
  - IEC 61968 & IEC 61970 series.
- Undertake the development of standards and/or technical reports on end-to-end security issues.

  End-to-End Security = a set of security policies, procedures, and technologies that provides a high degree of assurance that data exchanged between a source (sender) and a sink (receiver) is protected from unauthorized access and/or modifications, while being transferred from one end to the other through intermediate nodes.
- Addressed in currently 18+ parts of IEC 62351 of different status



[1] RBAC = Role-based Access Control

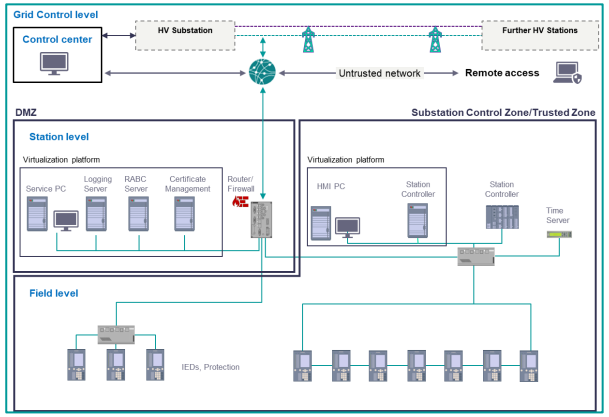
Cyber security is addressed in power system automation through IEC 62351

Building on state of the art security technology

IAM – Authentication, Identification Authorization (RBAC) of Users/Devices
Focus: Usage of X.509 certificates

Key management of long term and session keys
Focus: Application of established certificate management (EST, SCEP) and key management (GDOI) protocols

Secure communication between different actors (Ethernet, IP, serial)
Focus: Profiling of existing standards (e.g., TLS) and definition of security enhancements if necessary



Test case description for the specified security measures in the different parts of IEC 62351
Focus: Specification of conformity test cases

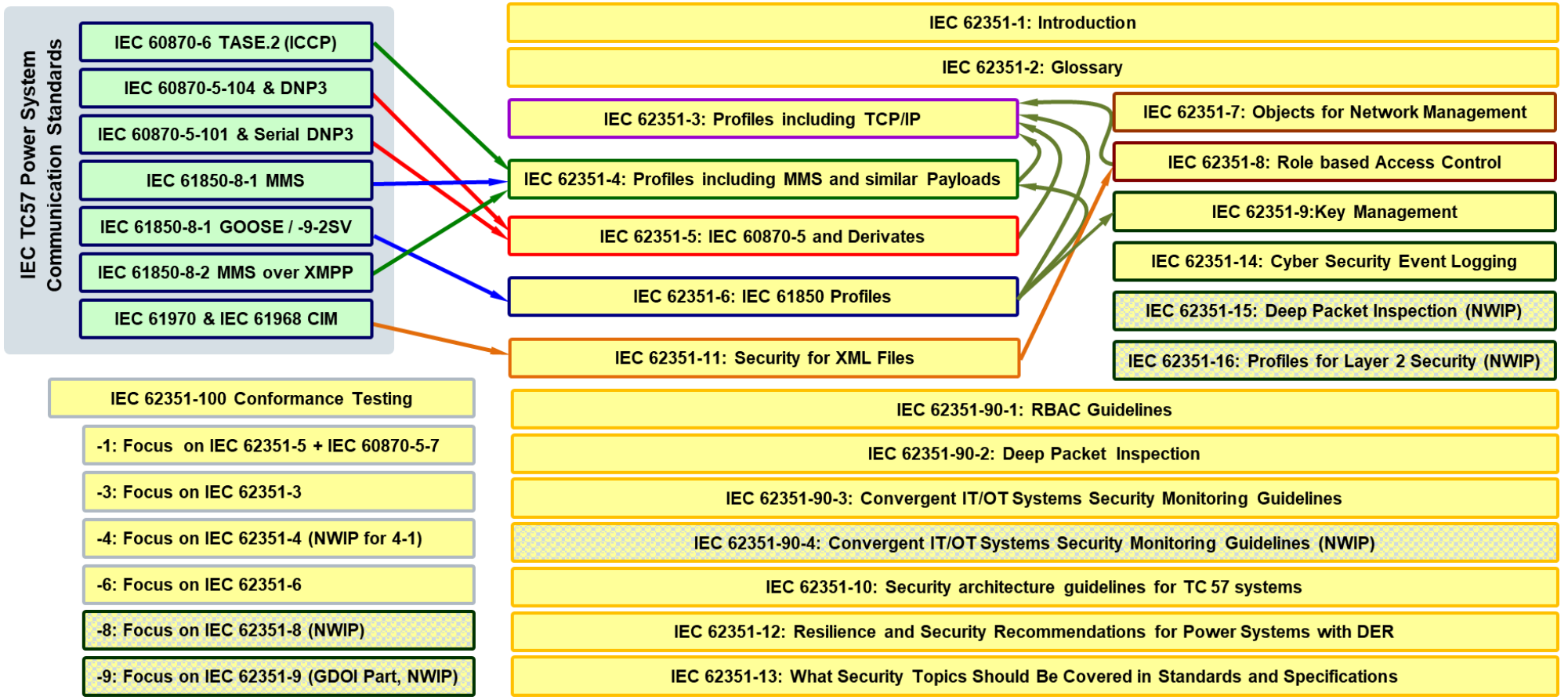
Monitoring and audit of security relevant events
Focus: Application of established standards like syslog and SNMP

Guidance and support for securing power system
Examples comprise role based access control (RBAC), Monitoring of communication connections, …

SIEMENS

Cyber security in Digital Grids

IEC 62351 provides technical security measures and guidelines



Security means defined for

- Authentication and authorization (RBAC)
- Secure IP- based and serial communication
- Secure application level exchanges
- Security monitoring and event logging
- Test case definition
- Guidelines for applying specific security measures

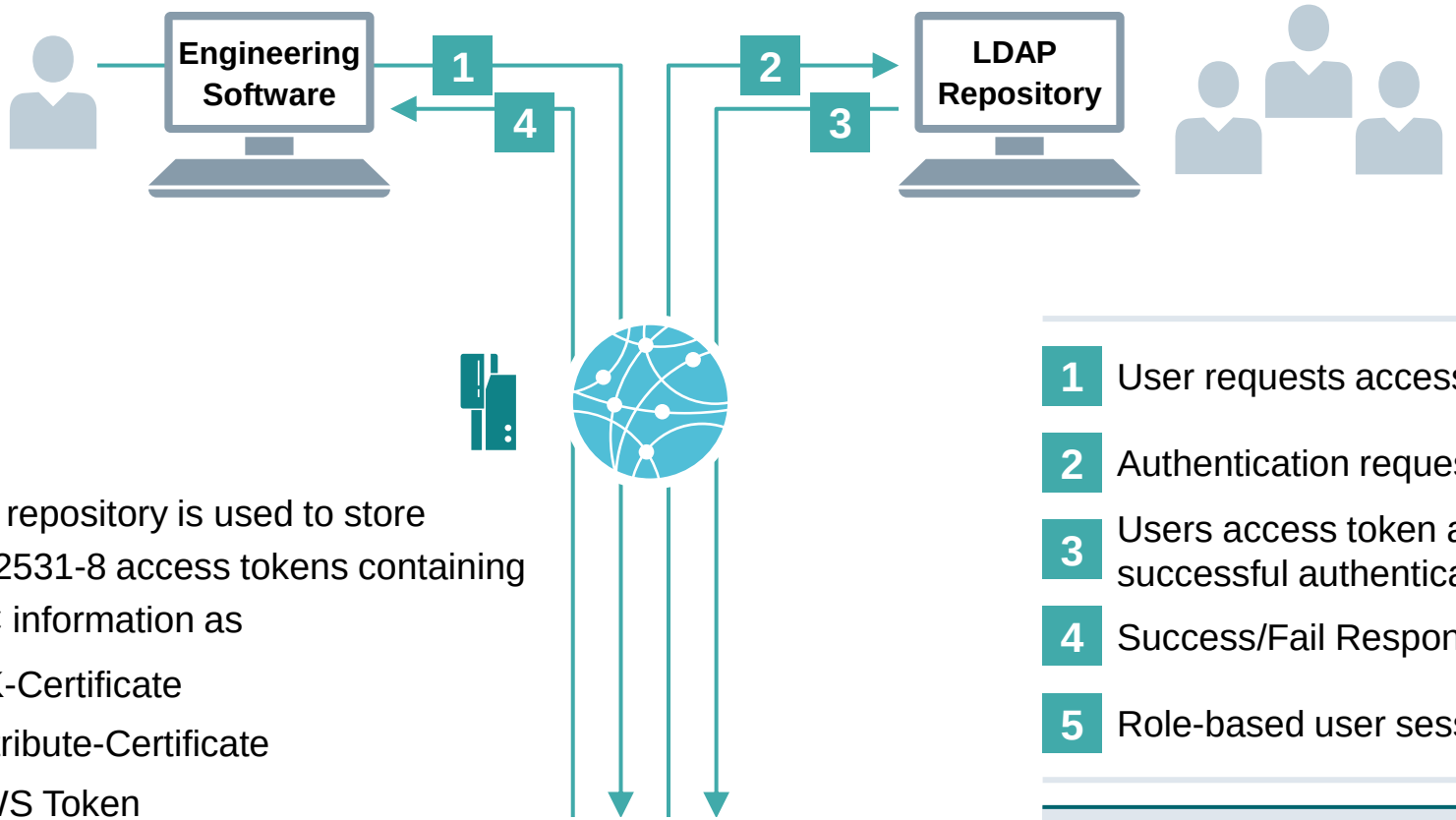
by utilizing or profiling

- existing standards and recommendations

SIEMENS

IEC 62351 Application Examples

Role-based access control to power systems and services with PULL



Roles ←→ Users	Role
User 1	Engineer
User 2	Admin
…	

LDAP repository is used to store IEC 62531-8 access tokens containing RBAC information as

- PK-Certificate
- Attribute-Certificate
- JWS Token

1. User requests access to IED with username and password
2. Authentication request with username, password via LDAP
3. Users access token as response from LDAP repository after successful authentication
4. Success/Fail Response from device to user
5. Role-based user session initiated/denied

Role to Permission mapping	Operation A	Operation B	Operation C	Operation …
Engineer	X	X		
Admin		X	X	
…				

SIEMENS

Different Security Standards meet in the Operational Environment

Application of IEC 62351 in a digital substation

Specification of technical solutions for an infrastructure supporting certificate based authentication and authorization (PKI, RBAC)

IEC 62351-8/9

Monitoring & Audit Adaptation and enhancement of existing infra-structures and technologies for network management using SNMP and syslog

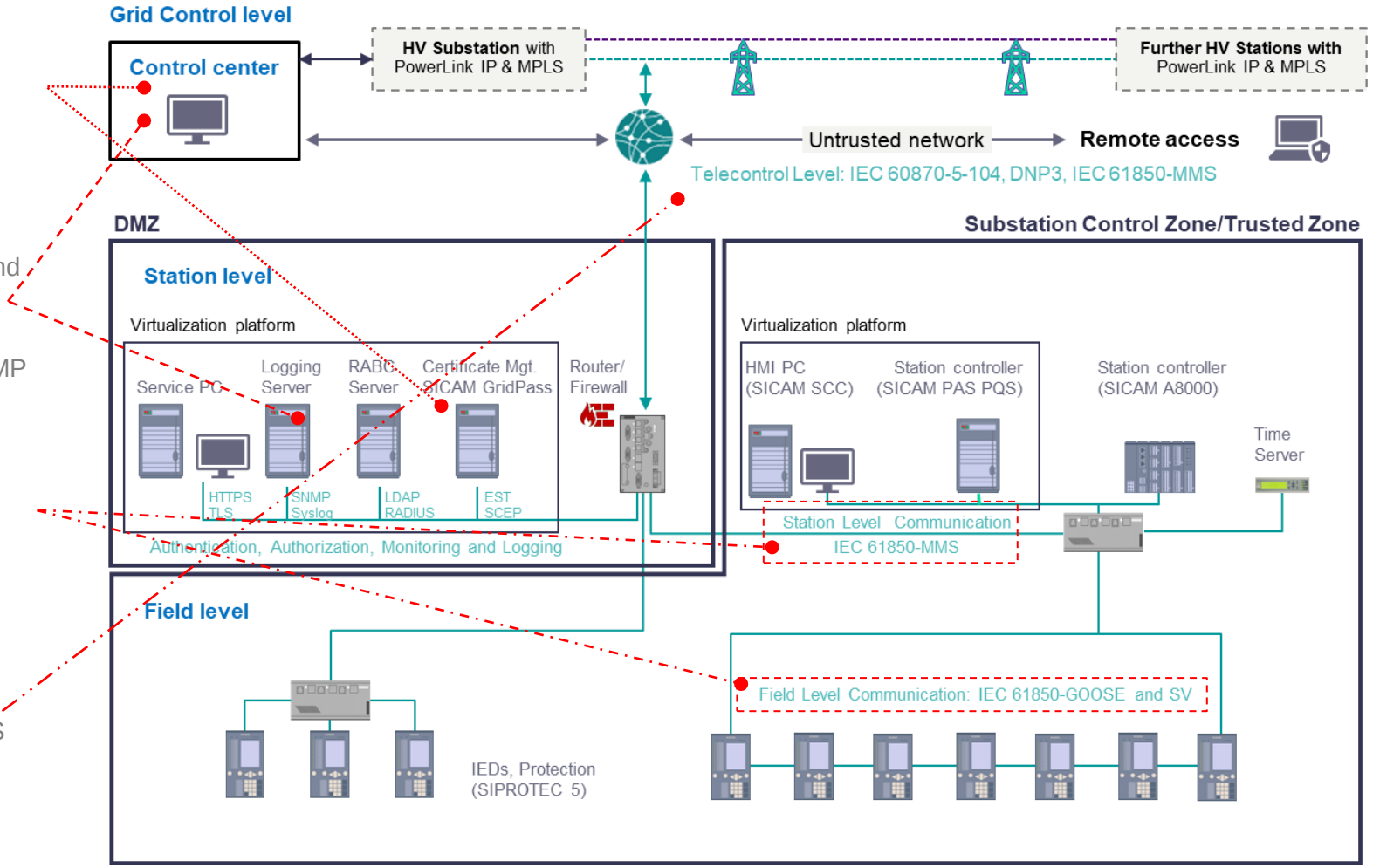
IEC 62351-7/14

Protection of process level and field level communication with real-time constraints using appropriate security measures

IEC 62351-3/4/5/6/9

Securing telecontrol and control center communication using TLS and / or security measures on application level

IEC 62351-3/4/5/9



Additionally, certification of security functionalities is possible to underline a security aware development and integration process as well as support of technical security means (e.g., using IEC 62351).

Certification possible according to IEC 62443


CERTIFICATE

No. IITS2 062845 0005 Rev. 00

Holder of Certificate: Siemens AG SI DG Humboldtstraße 59 90459 Nürnberg GERMANY

Site(s): Siemens AG SI DG EA-OP Humboldtstr. 59, 90459 Nürnberg, GERMANY

Certification Mark:

Product Type: Industrial IT Security

Model(s): Security Program for the "Blueprint Secure Substation"

Tested according to: IEC 62443-2-4:2015/AMD1:2017 IEC 62443-3-3:2013/COR1:2014 PPP 15011A:2018 (IEC 62443-2-4: Full Profile for a Control System)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 19CR12S020

Valid until: 2023-10-31

Date, 2020-11-04 (Christian Dirmeier)

Page 1 of 1 TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

SIEMENS

Security Requirement Consideration in Development and Feature Set definition on the example of a protection device

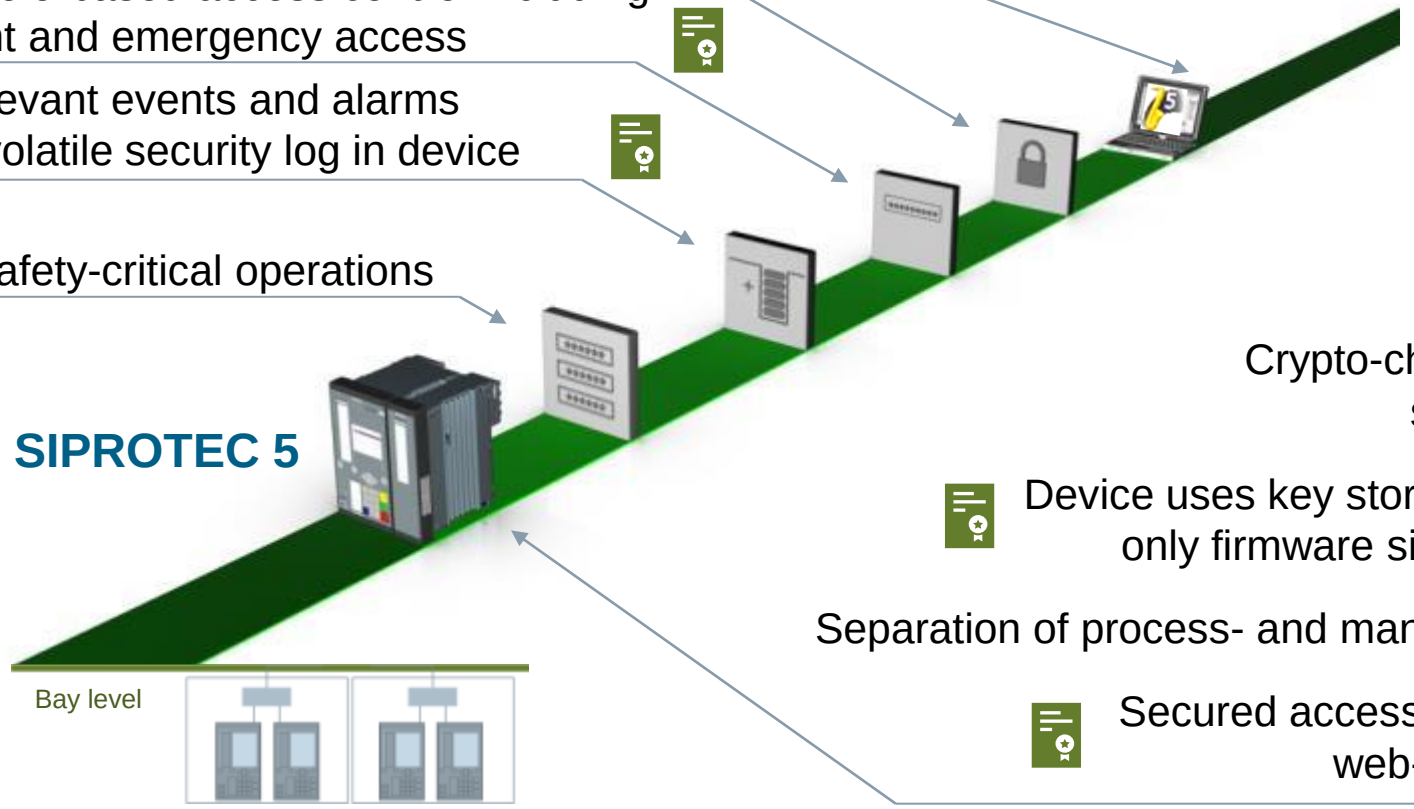
Technical Measures according to IEC 62351

Mutually authenticated and encrypted communication line for operational protocols and engineering

Device-side support for role-based access control including central user management and emergency access

Recording of security-relevant events and alarms over Syslog and in non-volatile security log in device

Confirmation codes for safety-critical operations



X.509 Certificates applied

Secure development
Patch management
Virus protection

Product hardening

Independent testing

Crypto-chip for secure information storage and transmission

Device uses key stored in crypto-chip to allow only firmware signed by Siemens to load

Separation of process- and management communication

Secured access for HMI interactions and web-based device monitoring

Measures for product lifecycle supported by requirements from IEC 62443

SIEMENS

Cybersecurity in the Power Grid
Security by Design in Products

Signed software/firmware

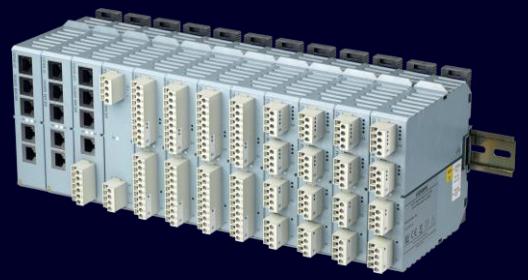
Protection against firmware/software manipulation

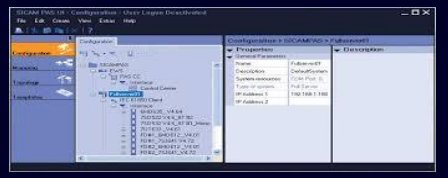
Firewall & VLAN

Separation of Ethernet traffic over integrated firewall & VLAN

Security Logging

Non-volatile persistence of security audit trail and transfer over Syslog





RBAC with central user management

Centrally manage users and assign roles for authorization (based on IEC 62351-8)

BDEW Whitepaper and IEC 62443 conformity

Fulfils recommendations for control and communication systems security

Certificate Management

Easy X.509 certificate management with SICAM GridPass

Gateway Features in SICAM A8000 & PAS

- VPN & TLS security
- Secure IEC 80670-5-104, IEC 61850, DNP3i
- Hardware-based application layer firewall in SICAM A8000
- Intrusion Detection

SIEMENS

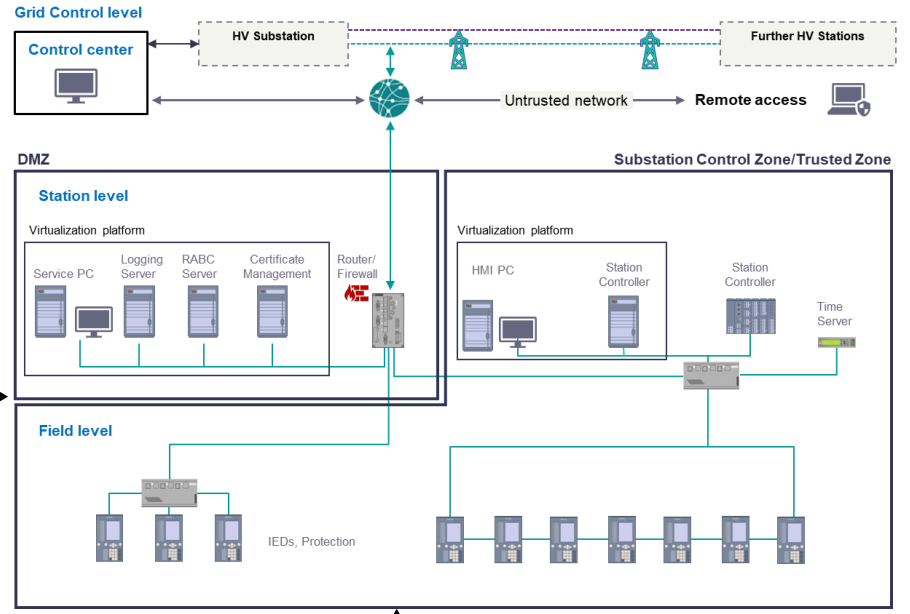
Cybersecurity for Power System Automation

Interplay of ISO/IEC 27001 / IEC 62443 / IEC 62351

Cyber Security regulation are provided for instance by
- European NIS Directive and derived country specific laws
- US FERC for North America

ISO/IEC 27001

Asset Owner Operator	IT Infrastructure	**ISO/IEC 27001**, **ISO/IEC 27019**
Integrator	IT Infrastructure	**IEC 62443-2-4**, **IEC 62443-3-3**, **IEC 62351**
Product Supplier	IT Infrastructure	**IEC 62443-3-3**, **IEC 62443-4-2**, **IEC 62443-4-1**, **IEC 62351**



Procedural: e.g.: ISMS for operator, or requirements for the development process for integrators and manufacturers

Functional: e.g., security levels, strength of security measures

Technical: e.g., security measures implementation, support interoperability

SIEMENS

All good?
Well, there are still Security Challenges!

- **Operational challenge** to migrate existing systems to utilize specified security standards and BCPs
- Observation of **System Integrity** to identify unauthorized (and also unintended) changes in system configuration. This may be connected with response handling upon detection.
- Ensuring **Resilience** to allow a system to stay operational with a degraded performance or functionality even when it has been attacked successfully.
- Performing **Monitoring** of industrial communication to ensure reliance with the intended operational environment even if the communication is encrypted. Influences on network design and privacy to be obeyed.
- Support of **Crypto Agility** to enable migration to stronger cryptographic algorithms. Advances in quantum computing endangers specifically asymmetric cryptographic algorithms like RSA or Elliptic Curve Cryptosystems (ECC) used for authentication, authorization, and key agreement in devices and infrastructure.
- Address **Supply Chain Security** requirements to enable verification of the system integrity along the product value chain and also after commissioning during operation.

SIEMENS

Summary & Outlook

- Cybersecurity has been acknowledged as prerequisite for limiting risks in critical infrastructures.
- Regulation increasingly requires to address technical and organizational cybersecurity measures to ensure reliable operation of critical infrastructures and beyond.
- Standardization and guideline activities support the alignment of approaches and interoperability of different vendor’s products and need to adopt upcoming new requirements.
- Security-by-Design is essential to provide appropriate security features from the ground and addresses functional requirements as well as procedural means during product manufacturing and operation.
- Cyber security needs a holistic approach – collaboration between vendors, integrators and operators; taking into account people, processes, and products in the specific domain.

- Still, some challenges remain and provide further food for thoughts.

SIEMENS

Contact

Steffen Fries
Principal Key Expert

T CST
Otto-Hahn-Ring 6
81739 Munich
Germany

E-mail steffen.fries@siemens.com

Siemens Grid Security

Siemens Cyber Security

SIEMENS

Information

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Security note

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic Industrial Security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art Industrial Security concept. Third-party products that may be in use should also be considered. For more information on Industrial Security, visit:

siemens.com/industrial-security

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit

support.automation.siemens.com

SIEMENS